**Amendments to the Claims:**

This Listing of Claims will replace all prior versions, and listings, of claims in the application. Compared to prior versions, claims 1, 3-58 and 90-101 are presented for examination. Claims 1, 20, 49, 50, 90 and 98 are amended while claim 2 is canceled and claims 59-89 remain withdrawn. All other claims (3-19, 21-48, 51-58, 91-97 and 99-101) remain as originally or previously presented.

**Listing of Claims:**

1. (Currently Amended) A computer server system for managing digital identity information, comprising at least one processor in operable connection with a memory configured by a database, the database including a vault for storage of ~~at least one~~ multiple user objects for [[a]] multiple users, the vault having access rights granted to a system administrator for management of the multiple user objects, each of the user objects having a corresponding safe object, the safe object containing ~~at least one~~ multiple different profiles accessed and administered exclusively by a single one of the multiple users at the exclusion of the system administrator, each profile including digital identity information provided by the single one of the multiple users and operable to be shared with other of the multiple users having other multiple different profiles accessible and administered exclusively by the other of the multiple users, the sharing occurring exclusively upon initiation by the single one of the multiple users.

2. (Canceled)

3. (Original) The system of claim 1, wherein the safe object also contains at least one user-administered contact, each contact representing an entity outside the user's safe

which receives controlled read access to digital identity information from at least one of the profiles.

4. (Original) The system of claim 1, wherein the safe object also contains at least one drop box object.

5. (Original) The system of claim 1, wherein the safe object also contains at least one application object with settings for an application.

6. (Original) The system of claim 1, wherein the safe object also contains at least one view object.

7. (Original) The system of claim 1, wherein the safe object also contains at least one access object.

8. (Original) The system of claim 1, wherein the system comprises a web server and an identity server.

9. (Original) The system of claim 8, wherein the web server and the identity server communicate using encrypted usernames.

10. (Original) The system of claim 8, wherein the web server and the identity server are secured by a firewall.

11. (Original) The system of claim 1, wherein the system comprises an identity server appliance.

12. (Original) The system of claim 1, further comprising a zero-byte client.

13. (Original) The system of claim 1, further comprising an installed client.

14. (Original) The system of claim 1, wherein the system comprises a provider model for access to the database, and the provider model abstracts the details of a particular directory and storage protocol.

15. (Original) The system of claim 1, wherein the system comprises an abstract model for access to the database, and the abstract model offers a hierarchical storage system in a representation that includes a user, a container, and data.

16. (Original) The system of claim 1, wherein the system comprises a programmatic interface to identity items and operations that correspond generally to directory service objects.

17. (Original) The system of claim 1, wherein the database includes multiple safe objects contained in a vault object.

18. (Original) The system of claim 17, wherein the system includes at least two vault objects hosted on different servers, each vault object contains at least one user safe object, and objects contained by the safe objects are federated to provide controlled access between the vault servers.

19. (Original) The system of claim 18, wherein the objects are federated using a Universal Resource Identifier which specifies at least a protocol, a host, a path, and an

object.

20. (Currently Amended) The system of claim 1, further comprising a digital business card application object having a corresponding profile object which includes digital identity information provided by the single one of the multiple users.

21. (Original) The system of claim 1, wherein the system comprises a means for one user to receive updated profile information of another user using a link to the database.

22. (Original) The system of claim 1, wherein the database is a partitioned directory services database.

23. (Original) The system of claim 1, wherein the system is further characterized in that it provides an account creation service which creates a new account for a user based on a template.

24. (Original) The system of claim 1, wherein the system is further characterized in that it provides a safe management service which provides an administrative tool to manage and maintain safe objects.

25. (Previously Presented) The system of claim 1, wherein the system is further characterized in that it provides a schema management service which permits the system administrator to at least view a directory service schema.

26. (Original) The system of claim 1, wherein the system is further characterized in that it provides a batch account creation service which creates several accounts at one time.

27. (Original) The system of claim 1, wherein the system is further characterized in that it provides an install service which permits one to install and configure an identity server.

28. (Original) The system of claim 1, wherein the system is further characterized in that it provides a backup and restore service which allows one to backup and restore at least one safe object.

29. (Original) The system of claim 1, wherein the system is further characterized in that it provides a safe advisor service which allows one to verify the integrity of a safe object.

30. (Original) The system of claim 1, wherein the system is further characterized in that it provides a legal recovery tool which recovers digital identity information for forensic use.

31. (Original) The system of claim 1, wherein the system is further characterized in that it provides a data denormalization service which facilitates data transformation on database fields.

32. (Original) The system of claim 1, wherein the system is further characterized in that it provides a rules service.

33. (Original) The system of claim 1, wherein the system is further characterized in that it provides an event service which allows an identity server to register interest in and be notified of changes in the database.

34. (Original) The system of claim 1, wherein the system is further characterized in that it provides an identity verification service which allows one to verify the identity of a user based on registration information.

35. (Original) The system of claim 1, wherein the system is further characterized in that it provides an authorization service which allows a process to verify information gathered from a user registration form.

36. (Original) The system of claim 1, wherein the system is further characterized in that it provides a profile discovery and publishing service which allows users to publish at least a portion of their profile information.

37. (Original) The system of claim 1, wherein the system is further characterized in that it provides a form fill-in service which allows a user to have the service fill in at least part of an online form with information from one of the user's profile objects.

38. (Original) The system of claim 1, wherein the system is further characterized in that it provides a form conversion service which assists a webmaster in converting existing forms to standardized field names.

39. (Original) The system of claim 1, wherein the system is further characterized in that it provides an install service which installs servlets on a web server.

40. (Original) The system of claim 1, wherein the system is further characterized in that it provides an identity exchange service for portions of a privacy protection protocol.

41. (Original) The system of claim 1, wherein the system is further characterized in that it provides a chat service which sets up chat rooms so users can communicate with each other in real time.

42. (Original) The system of claim 1, wherein the system is further characterized in that it provides a presence service which lets users specify where they are and allows them to discover another user's presence information.

43. (Original) The system of claim 1, wherein the system is further characterized in that it provides an anonymous remailer service which allows users to choose different email addresses for different profiles.

44. (Original) The system of claim 1, wherein the system is further characterized in that it provides an anonymous browsing service which allows a user to browse a network in an anonymous fashion to prevent sites from collecting user identity information.

45. (Original) The system of claim 1, wherein the system is further characterized in that it provides an infomediary service which facilitates creating an infomediary.

46. (Original) The system of claim 1, wherein the system is further characterized in that it uses profile objects and software for tracking IP addresses in order to selectively publish the last known IP address of a user.

47. (Original) The system of claim 1, wherein the system is further characterized in that it uses profile objects and at least one of an underlying directory service and an underlying file system in order to enforce access controls on web pages published by users.

48. (Original) The system of claim 1, wherein the system is further characterized in that it provides email services.

49. (Currently Amended) The system of claim 48, wherein the single one of the multiple users has an email address, and the system encodes contact relationship information in the ~~user's~~ email address.

50. (Currently Amended) The system of claim 48, wherein the system uses profiles to filter email sent to the single one of the multiple users.

51. (Original) The system of claim 1, further comprising a means for determining whether a user logging in at a third party web site is registered as a user of the system.

52. (Original) The system of claim 51, further comprising a means for logging the user into the system if the user is registered, and a means for registering the user and logging the user in if the user was not registered.

53. (Original) The system of claim 52, wherein the means for registering the user and logging the user in comprises a means for capturing user login information for the third party web site.

54. (Original) The system of claim 1, wherein the system is further characterized in that user digital identity information is only made available to a partner site if the user has flagged the information as public.

55. (Original) The system of claim 1, wherein the system is further characterized in that it uses an embossed icon which provides a transaction history.

56. (Original) The system of claim 1, wherein the system is further characterized in that it uses an embossed icon which provides a user authentication mechanism.

57. (Original) The system of claim 1, wherein the system is further characterized in that it uses an embossed icon which provides a launch point for launching application programs.

58. (Previously Presented) The system of claim 1, wherein the system is further characterized in that it uses a non-repudiation feature whereby the system administrator cannot change a user password and then log on as the user.

Claims 59-89 (Withdrawn)

90. (Currently Amended) A computer server system for managing digital identity information, comprising one or more processors in operable connection with one or more memories defining a vault for storage of one or more safes of digital identities, the vault including an access protocol layer, an identity server layer and an identity manager layer and having access rights granted to one or more system administrators including management of the one or more safes of digital identities of one or more accounts of end users, the one or more safes of digital identities having multiple profiles each with access rights granted exclusively to the end users via the one or more accounts including the exclusion of access rights of the one or more system administrators, the multiple profiles being shared amongst the end users at the exclusion of the one or more system administrators.

91. (Original) The system of claim 90, wherein the access protocol layer includes one or more protocols selected from LDAP, XML, RPC-over-HTTP, XDAP or SMTP.

92. (Original) The system of claim 90, wherein the identity server layer serves as an NDS access point.

93. (Original) The system of claim 90, wherein the identity server layer maintains access rights to the digital identities.

94. (Original) The system of claim 90, wherein the identity manager layer includes NDS authentication and authorization that controls access to the digital identities.

95. (Original) The system of claim 90, wherein the identity manager layer has a secret store.

96. (Original) The system of claim 90, wherein the one or more processors and the one or more memories are located on an identity server.

97. (Original) The system of claim 90, wherein the one or more processors and the one or more memories are functionally apportioned between a client, a web server and an identity server, including servlets and applets.

98. (Currently Amended) A configured computer-readable storage medium that manages digital identities, comprising a vault for secure storage of one or more safes of digital identity profiles, the vault having an access protocol layer, an identity server layer and an identity manager layer and having access rights granted to a system administrator for management of the safes of digital identity profiles, the one or more safes of digital identity profiles having access rights granted exclusively to one or more end users at locations remote from the vault, the one or more safes of digital identity profiles further including multiple profiles shared amongst the end users at the exclusion of the system administrator.

99. (Original) The configured storage medium of claim 98, further including a zero-byte client interface.

100. (Original) The configured storage medium of claim 98, further including a client application interface.

101. (Previously Presented) The configured storage medium of claim 98, further including a database including a user object and a corresponding safe object, the safe object containing at least one profile of the digital identity profiles.